GOVERNMENT SURVEILLANCE AND INDIVIDUAL FREEDOM: A PROPOSED STATUTORY RESPONSE TO LAIRD v. TATUM* AND THE BROADER PROBLEM OF GOVERNMENT SURVEILLANCE OF THE INDIVIDUAL

GEORGE C. CHRISTIE**

The term "surveillance" has taken on symbolic significance in our times. To those who shout "law and order" and decry the pampering of criminal defendants, surveillance is viewed as an essential law enforcement tool. To those who stress the protection of individual freedoms and point to the embattled position of a criminal defendant struggling against the monolithic forces of the state, surveillance is cast as an ugly instrument of repression. Of course, when considered in the abstract, both of these are extreme positions, and the Congress has at least attempted to define appropriate legal parameters for the use of electronic surveillance. But in the wider domain of surveillance of the public acts of individuals—whether by the military or the civilian law enforcement agencies—no legal guidelines have been drawn. In this article, Professor Christie suggests a solution to this broader issue by proposing a federal statute which delineates those circumstances in which surveillance in its broadest sense is warranted. In structuring his statute, the author makes an effort to balance the seemingly conflicting objectives of those who emphasize society's need for security and those who emphasize the individual's need for privacy.

I

INTRODUCTION

The American people were no doubt shocked to learn of the surveillance of civilians in recent years—particularly in 1968—by undercover agents of the United States Army. Many of the details behind these surprising revelations were brought to light in the important hearings conducted by Senator Ervin's Subcommittee on Constitutional Rights in the spring of 1971. Although the surveillance was ostensibly justified by the Government's

* 408 U.S. 1 (1972).
** Professor of Law, Duke University School of Law.
1 This concern can even be seen in Chief Justice Burger's majority opinion in Laird v. Tatum, 408 U.S. 1, 15-16 (1972).
2 Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 92d Cong., 1st Sess. (1971). [These hearings were printed in two parts and will be hereinafter referred to as Hearings Pt. I and Hearings Pt. II.] See generally Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, Staff Report, Army Surveillance of Civilians: A Documentary Analysis, 92d Cong., 2d Sess. (1972) [hereinafter Staff Report].
legitimate need to secure advance information on possible civil disturbances, it is now public knowledge that the Army engaged in surveillance during political rallies and that it maintained files on candidates for public office including persons who are now members of the United States Senate and the United States House of Representatives. Similarly, it has been divulged that the Army has monitored lectures given at various universities. While the Army has maintained that it was only fulfilling the request of the civil authorities for help in law enforcement, those subjected to much of this surveillance could by no stretch of the imagination be considered potential criminals. In testimony presented before Senator Ervin's subcommittee, senior officials stated that the Department of the Army had essentially ceased all such activities in June of 1970 and that the Department now relies primarily upon the Federal Bureau of Investigation (FBI) and the Internal Security Division of the Department of Justice for the performance of all such functions. While the withdrawal of the Army from these types of activities is a beneficial development—both from the point of view of the Army and the American people, since such activities are hardly germane to the Army's mission—it falls far short of the sweeping type of fundamental reform that is needed. Moreover, as shall soon be seen, the Department of Defense still claims some authority to engage in the surveillance of civilians.

But surveillance by the military is only one part of the problem. The Government has continued to maintain that it has a virtually

---

8 See Statement by R.F. Froehlke, Assistant Sec'y of Defense (now Sec'y of the Army), Hearings Pt. 1, supra note 2, at 375-85.
9 Id. at 389.
10 Statement by C.H. Pyle, former Captain, Army Intelligence, id. at 161; statement by L.F. Lane, former Army Intelligence agent, id. at 314.
11 Id. at 394; statement by W.H. Rehnquist, Asst. Att'y General, Office of Legal Counsel (now Associate Justice, United States Supreme Court), id. at 601.
12 One might note in this regard that the use of Army personnel as a personam comitatus, except where "expressly authorized by the Constitution or Act of Congress," is made a crime by 18 U.S.C. § 1385 (1970). In 10 U.S.C. §§ 331-34 (1970), Congress has narrowly limited the occasions on which the military may be used for law enforcement purposes: suppressing insurrection upon request of the legislature or governor of a state, id. § 331; enforcement of federal authority, id. § 332; and the suppression of domestic violence or unlawful combinations or conspiracies that hinder the execution of state and federal law and result in deprivation of constitutional rights or that obstruct the execution of the laws of the United States, id. § 333. In all of these cases, Presidential action is required, including a Presidential proclamation ordering the "insurgents to disperse and retire peaceably to their abodes within a limited time." Id. § 334.
13 See text accompanying notes 37-52 infra.
unlimited right to engage in the surveillance of American citizens, at least when that surveillance does not involve wiretapping or other forms of possibly unlawful intrusion. In pursuit of that policy, for example, the FBI engaged in general surveillance at the Earth Day Rally held in Washington, D.C., on April 22, 1970, at which Senator Muskie was one of the speakers. In response to the justified fears of the American people as to the potentially far-reaching sweep of such surveillance activities, the Administration has declared that the American people must rely on the "self-discipline . . . of the Executive branch" to insure that the Government's right of surveillance is not abused. The Government has not, however, informed the American people of the exact nature of its surveillance policies. Specifically, it has not told the American people how it determines who is a legitimate subject of surveillance nor has it advised the American people what criteria, if any, it uses in deciding when to terminate the surveillance of a particular individual or group once the surveillance has begun.

In 1968, Congress made a limited effort to regulate the surveillance activities of the Government when it granted the Government limited powers of electronic surveillance. In Title III of the Omnibus Crime Control and Safe Streets Act, Congress authorized the Attorney General and, where permitted by state law, appropriate state officials to seek court orders for the seizure of wire or oral communications when there is reasonable cause to believe that these communications relate to certain specified serious crimes. The requirement of a court order is dispensed with only in cases involving an exercise of the President's power to protect the United States against attack by foreign powers, to protect against the overthrow of the Government by force, to protect against other clear and present dangers to the structure and existence of the Government or to obtain essential foreign intelligence information—and then only if the President has authorized the seizure of the communications. In all other sittua-

---

10 Statement by W.H. Rehnquist, Hearings Pt. I, supra note 2, at 597.
11 Speech by Senator Edmund Muskie on April 14, 1971, on the floor of the Senate at the conclusion of which he inserted into the Congressional Record the FBI report on its surveillance at the Earth Day activities, 117 Cong. Rec. 10,313 (1971). See generally Hearings Pt. II, supra note 2, at 1583.
12 Statement by W.H. Rehnquist, Hearings Pt. I, supra note 2, at 603.
15 Id. § 2511(3). For minor exceptions, however, such as consent, see id. § 2511(2).
tions, court orders are not only required but, with one exception, must be obtained before the electronic surveillance commences.\textsuperscript{10} This exception allows surveillance to begin prior to obtaining a court order in emergency situations involving national security or organized crime, provided that application for a court order is made within forty-eight hours.\textsuperscript{17}

On its face, of course, this purported regulation does not seem to be much of a limitation of the Government's surveillance activities because, prior to the Act, some forms of electronic surveillance by government officials, such as wiretapping, were already arguably illegal.\textsuperscript{18} The fruits of such surveillance, moreover, were not admissible as evidence against the accused in the federal courts\textsuperscript{10} and, in later years, in the state courts as well.\textsuperscript{20}

\textsuperscript{10} Id. § 2518.

\textsuperscript{17} Id. § 2518(7). For a critical discussion of the developments which culminated in the "national security" exception, see Theoharls & Meyer, The "National Security" Justification for Electronic Eavesdropping: An Elusive Exception, 14 Wayne L. Rev. 749 (1968).

\textsuperscript{18} Section 605 of the Federal Communications Act of 1934, Act of June 19, 1934, ch. 652, § 605, 48 Stat. 1163, as amended 47 U.S.C. § 605 (1970), provided that "no person not being authorized by the sender shall . . . divulge or publish the existence, contents, substance, purport, effect, or meaning" of an interstate or foreign wire or radio communication. There was an exception to cover the normal chain of communication, e.g., telegraph company employees. Id. Among its other prohibitions the Act also provided that "no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same . . . for his own benefit" or for the benefit of someone else. Id. Section 605 was interpreted by the Supreme Court to bar the use of wiretap evidence in the federal courts. Nardone v. United States, 302 U.S. 379 (1937). The Department of Justice, however, interpreted § 605 to allow wiretapping so long as the wiretap information was not divulged outside of the Department. See, e.g., Brownell, The Public Security and Wire Tapping, 39 Cornell L.Q. 195 (1954); Rogers, The Case for Wire Tapping, 63 Yale L.J. 792 (1954). This view was sharply criticized on the grounds that the "use" made of such wiretap information by the Department of Justice, even though it is within the Department, is a "use" prohibited by the statute and that divulgence of such information, even within the Department, is divulgence under the statute and likewise prohibited. See, e.g., Donnelly, Comments and Caveats on the Wire Tapping Controversy, 63 Yale L.J. 799 (1954); Williams, The Wiretapping-Eavesdropping Problem: A Defense Counsel's View, 44 Minn. L. Rev. 855 (1960). Wiretapping activities have in recent years also been subjected to constitutional scrutiny. See notes 19-20 infra.

\textsuperscript{10} Nardone v. United States, 302 U.S. 379 (1937), held that wiretap evidence is inadmissible in a federal prosecution. This holding was extended in the second Nardone case, Nardone v. United States, 308 U.S. 338 (1939), to exclude the fruits of wiretap evidence as well. The Supreme Court has since held that telephone conversations can be the subject of searches and seizures and that they are entitled to the protection afforded by the fourth and fourteenth amendments, Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967); cf. Alderman v. United States, 394 U.S. 165 (1969).

\textsuperscript{20} Two days before the electronic surveillance provisions of the Omnibus Crime Control and Safe Streets Act of 1968 were signed into law, the Supreme Court held that § 605 of the Federal Communications Act of 1934 prohibited

Imaged with the Permission of N.Y.U. Law Review
On the other hand, since wiretapping and other types of electronic surveillance were in fact frequently utilized by law enforcement agencies, the controls introduced by the Act were undoubtedly a step in the right direction. Furthermore, the Act covers other forms of electronic surveillance aside from wiretapping and the "bugging" of homes and offices, and it provides for civil as well as criminal penalties for violations. This does not mean, however, that the Act is not subject to justifiable criticism or that it provides the maximum possible protection to the individual.

Nevertheless, the Government has not been satisfied with the authority granted it by the Omnibus Crime Control and Safe Streets Act. In United States v. United States District Court for the Eastern District of Michigan, it claimed that the President's constitutional power to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government—

—which the Act disclaims any intention of impinging—includes the inherent right to tap the telephones of private citizens, without bothering to secure a warrant either before or after the event, whenever the Attorney General deems it in the interests of the national security. The Supreme Court, fortunately, unanimously rejected this contention. All that most of the Justices were prepared to concede to the Government was the power of Congress to provide for a different type of procedure for securing warrants to take into account the special circumstances of national security cases. A warrant there must be, however, if such surveillance is to withstand challenge under the fourth amendment.

In the broader area of general surveillance, however, the Congress has thus far not acted, and it is in this area that the Government claims the broadest powers. That the existence of such

---

22 See id. §§ 2511, 2520.
26 407 U.S. at 320.
27 Id. at 322-34.
broad investigative powers can have a very disturbing inhibiting effect on the exercise of the freedoms of speech and association that it is the purpose of government to protect cannot be doubted.\textsuperscript{28} Nor can one ignore the threat to human dignity if the individual can never be sure that he is not under government surveillance whenever he walks the public streets. These fears are by no means completely chimerical. It is a known fact, for example, that the Department of Justice maintains files on well over 10,000 so-called "subversives," many of whom have never been charged with a crime.\textsuperscript{29} The existence of such files, when coupled with broad claims about the power to engage in surveillance, represents a serious inroad upon the privacy of the individual.

Concerned individuals have now started to turn to the courts to secure protection against the official exercise of these broad powers that the Department of Justice and some local police authorities claim are the inherent right of law enforcement agencies.\textsuperscript{30} However, the most widely publicized challenge, \textit{Laird v.}

\textsuperscript{28} I have consciously avoided using the term "chilling effect" because it has become a term of art in constitutional litigation. I am not here concerned with the question of whether the Constitution protects the individual from government surveillance of his public activities. (In this regard, however, see note 68 infra.) I am alluding rather to the well-documented fact that people are concerned about government intrusions through surveillance and data collection into the privacy of their lives. See Hearings Pts. I & II, supra note 2; A. Miller, The Assault on Privacy (1971). See also Askin, Surveillance: The Social Science Perspective, 4 Colum. Human Rights L. Rev. 59 (1972); Ervin, Privacy and Government Investigations, 1971 Ill. L.F. 137; Note, Police Surveillance of Political Dissidents, 4 Colum. Human Rights L. Rev. 101 (1972); Note, Police Use of Remote Camera Systems for Surveillance of Public Streets, id. at 143.

\textsuperscript{29} See N.Y. Times, Apr. 2, 1971, at 25, col. 3; Washington Post, June 13, 1971, § A, at 1, col. 1. See also Washington Post, July 4, 1971, § A, at 1, col. 1. While the existence of such files received increased attention in the late 1950's (when black power groups began to appear), the Washington Post article of June 13, 1971, supra, written by William Greider, makes it clear that such files on politically suspect persons have been kept since at least the 1930's, and possibly earlier. In a similar vein, one might also note the statement of L. Patrick Gray, the Acting Director of the FBI, that the Bureau will no longer compile "biographical data" on "major candidates" for Congress. N.Y. Times, Oct. 28, 1972, at 1, col. 1.

\textsuperscript{30} See Anderson v. Sills, 56 N.J. 210, 265 A.2d 678 (1970). This suit, which was ultimately largely unsuccessful, was brought for declaratory and Injunctive relief against the use of a reporting system claimed to have been instituted at the behest of the New Jersey Attorney General in the form of a memorandum to local and state officials entitled "Civil Disorders—the Role of Local, County and State Government." Certainly, as the short-lived lower court decision observed, the range of possible surveillance—there was no evidence that actual surveillance had gone that far—would cover most forms of political activity. Anderson v. Sills, 160 N.J. Super. 545, 555-57, 256 A.2d 298, 304 (Ch. 1969), rev'd, 56 N.J. 210, 265 A.2d 678 (1970). More recently, it was reported that United States District Court Judge Constance Baker Motley of the Southern District of New York issued an injunction against the New Rochelle, New York police to stop the sur-
Tatum, was against the Army’s surveillance activities, whose nature has already been briefly described. Although the plaintiffs were unable to show that they were the subject of any particular acts of surveillance, they maintained that, given their roles as social activists, the mere existence of the Army’s surveillance activities had a chilling effect on the exercise of their first amendment rights. Though a divided court of appeals had held that the plaintiffs were entitled to try to prove their case by showing that the Army’s surveillance system did in fact derogate from their first amendment rights, the Supreme Court, in a five-to-four decision, reversed. In a majority opinion written by Chief Justice Burger, the Court held that the plaintiffs lacked standing to bring suit because of the absence of any concrete allegation of injury. The Court opined, however, that the subject was one peculiarly appropriate for congressional regulation.

The question of the correctness of the Court’s decision that Tatum and his colleagues lacked standing is beyond the scope of this discussion. Rather, the purpose of this article is to take up the suggestion of the Court and to propose a statutory scheme not only for the regulation of surveillance by the military but also for the vastly greater and—in practice—more important problem of surveillance by the Government’s civilian law enforcement agencies. The latter aspect of the proposed statute (i.e., the attempt to regulate the surveillance of civilian law enforcement authorities) is all the more significant since the only legislative effort to cope with the general problem of surveillance to date—Senator Ervin’s recent bill—deals only with military surveillance. In order to assist the reader in his evaluation of the proposed statute, which appears in Part IV of this article, the intervening discussion

veilance of persons “neither suspected of criminal activity nor engaged in criminal activity.” N.Y. Times, June 23, 1971, at 47, col. 8. For a final illustration, see Donehoo v. Dulles, 330 F. Supp. 308 (E.D. Va. 1971), aff’d, 465 F.2d 196 (4th Cir. 1972), a decision in which demonstrators who admitted they had actively sought media coverage of their activities were denied an injunction which sought to prevent police from taking their photographs. This case and its subsequent history are discussed in note 69 infra. See also Yaffe v. Powers, 454 F.2d 1362 (1st Cir. 1972); Aronson v. Giarrusso, 456 F.2d 955 (5th Cir. 1972).


32 408 U.S. at 10.

33 Tatum v. Laird, 444 F.2d 947 (D.C. Cir. 1971).

34 408 U.S. at 13.

35 Id. at 15.

36 S. 3750, 92d Cong., 2d Sess. (1972); see text accompanying note 53 infra.
will focus on the considerations that underlie the major provisions of the proposal.

II

SURVEILLANCE BY THE MILITARY

A. Present Efforts to Deal with the Problem

1. DoD Directive 5200.27: An Attempt by the Military to Curtail Its Own Surveillance Activities

As has already been noted, the Army claimed before Senator Ervin's subcommittee that it has largely discontinued its surveillance activities. Specifically, on June 9, 1970, the Army adopted a policy of relying upon the Department of Justice, at the national level, for "civil disturbance planning, threat, and early warning information." Army intelligence resources, under this policy, were not to be used for the collection of civil disturbance information unless a determination was made at a responsible level that there was a distinct threat of civil disturbance beyond the capability of local and state authorities to control. Even then, collection efforts were to be limited to liaison activities. Overt collection, other than liaison, required approval by Army headquarters, and covert intelligence required the concurrence of both the FBI and the Under Secretary of the Army.

Subsequent to these actions by the Army, the Department of Defense entered the field and assumed overall responsibility for surveillance activities. In February of 1971, an Assistant Secretary of Defense was designated to act for the Secretary of Defense in all Defense Investigative Program matters. A Defense Investigative Review Council, consisting of senior Defense Department officials and senior civilian officials from the Army, Navy, and Air Force, was established to assist this Assistant Secretary to formulate policy guidance and to review current procedure in investigatory and related counterintelligence activities.

---

87 See text accompanying note 7 supra.
89 Id.
90 Id.
91 Id. It is worthy of note that in March 1970 the Army ordered the destruction of the computerized files that contained the results of the surveillance which was the gravamen of the plaintiffs' claim in Laird v. Tatum.
92 Department of Defense Directive 5200.26, Feb. 17, 1971, reprinted in Hearings Pt. II, supra note 2, at 1251. Originally, the authority was delegated to the Assistant Sec'y for Administration, but it is now delegated to the Assistant Sec'y (Comptroller). See Memorandum from the Sec'y of Defense of Dec. 29, 1971, reprinted in Hearings Pt. II, supra note 2, at 2088.
Department of Defense is now apparently also in the process of centralizing operational control of many of the investigatory activities of the military departments. 44

One of the first actions of the Defense Investigative Review Council was to consider a proposed directive concerning the acquisition of information about persons not affiliated with the Department of Defense. 45 Shortly after the Council was established, the proposed directive was issued as Department of Defense Directive 5200.27 (DoD Directive 5200.27), which was to be effective as of March 1, 1971. 46 This directive provided, for the first time, general policy, procedures and operational guidance for all components of the Department of Defense. The directive prohibits "collecting, reporting, processing, or storing information on individuals . . . not affiliated with the Department of Defense" except where "essential" to the performance of the following missions of the Department of Defense: (1) "Protection of [Department of Defense] functions and [p]roperty"; (2) "[p]ersonnel security"; and (3) "[o]perations related to civil disturbance." 47

In performing the first mission, "Protection of [Department of Defense] functions and [p]roperty," surveillance activities are permitted only in instances involving: (1) subversion of discipline, loyalty and morale of military and civilian personnel "by actively encouraging violation of law, disobedience of lawful order or regulation, or disruption of military activities"; (2) "theft of arms and ammunition"; (3) "acts jeopardizing the security of Department of Defense elements or operations or compromising classified information by unauthorized disclosure or by espionage"; (4) unauthorized demonstrations on Department of Defense installations; (5) direct threats to military and Department of Defense civilian personnel or persons authorized protection by the Department of Defense; (6) activities endangering facilities engaged in classified defense contracts or which have been designated key defense facilities; and (7) crimes for which the Department of Defense has prosecutorial or in-

46 Id. The text of Department of Defense Directive 5200.27 [hereinafter DoD Directive 5200.27] is reprinted in Hearings Pt. II, supra note 2, at 1253. (A copy of this and other Department of Defense directives may be obtained free of charge from the U.S. Naval Publications and Forms Center, 5501 Tabor Avenue, Philadelphia, Pa. 19120. They are not generally published in the Federal Register.)
47 DoD Directive 5200.27, supra note 46, III, IV.
vestigatory responsibility. With respect to the Department's second mission, "[p]ersonnel security," surveillance of certain categories of persons is permitted, including "DoD civilian personnel and applicants for such status" and those who seek access to classified information under various Department of Defense programs. Finally, with regard to the Department's third mission, "[o]perations related to civil disturbance," surveillance may be undertaken to secure "essential" information, provided that specific prior authorization by the Secretary or his designee has been obtained. Such authorization may only be granted when "there is a distinct threat of civil disturbance exceeding the law enforcement capabilities of state and local authorities.

After delimiting those circumstances in which surveillance may be engaged in by Defense Department personnel, the directive attempts to limit the possible abuse of that authority. In a section entitled "Prohibited Activities," certain restrictions are imposed on all surveillance activities undertaken in support of any of the three missions. The text of these restrictions provides:

A. The acquisition of information on individuals or organizations not affiliated with the Department of Defense will be restricted to that which is essential to the accomplishment of assigned Department of Defense missions under this Directive.
B. No information shall be acquired about a person or organization solely because of lawful advocacy of measures in opposition to Government policy.
C. There shall be no physical or electronic surveillance of Federal, state, or local officials or of candidates for such offices.
D. There shall be no electronic surveillance of any individual or organization except as authorized by law.
E. There shall be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary of Defense or his designee.
F. No DoD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information the collection of which is authorized by this Directive without specific prior approval by the Secretary of Defense or his designee. An exception to this policy may be made by the local commander concerned, or higher authority, when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In each such case a,

---

48 Id. IV(A).
49 Id. IV(B).
50 Id. IV(C). Various officials are delegated authority as the Secretary's designee to implement the sundry portions of the directive. They are all senior officials, and the directive provides that in no event can redelegation be made below the level of Under Secretary of the Service Departments. Id.
51 Id.
report will be made immediately to the Secretary of Defense or his
designee.

G. No computerized data banks shall be maintained relating to
individuals or organizations not affiliated with the Department
of Defense, unless authorized by the Secretary of Defense or his
designee.53

2. The Ervin Bill

On June 27, 1972, while this article was in the process of
preparation, Senator Ervin introduced Senate Bill 3750 to deal
with military surveillance of civilians.54 The crucial section of
the bill is section 3. It provides that

notwithstanding the provisions of the preceding section [which pro-
hibits, under pain of criminal sanction, surveillance of civilians by
the military] . . . it shall not be unlawful to use the land or naval
forces of the United States or the militia of a State (a) to do
anything necessary or appropriate to enable such forces or militia
to accomplish their mission after they have been actually and
publicly assigned by the President to the task of repelling invasion
or suppressing rebellion, insurrection, or domestic violence pursuant
to the Constitution or Section 331, Section 332, or Section 333 of
title 10 of the United States Code, or (b) to protect real or per-
sonal property committed to the custody of the land or naval
forces of the United States or the militia of any State from destruc-
tion, damage, theft, unlawful seizure, or trespass, or (c) to deter-
dine whether the employment or retention in employment of any
individual seeking or enjoying employment by the land or naval
forces of the United States or the militia of any State or in any
defense facility is consistent with the interests of national security.

Because of the late date of introduction, no action was taken on

53 Id. V. Mention should be made that paragraph (D) of part VI on "Op-
   erational Guidance" provides:
   Information within the purview of this Directive, regardless of when ac-
   quired, shall be destroyed within 90 days unless its retention is required
   by law or unless its retention is specifically authorized under criteria estab-
   lished by the Secretary of Defense or his designee.

With regard to existing records, the Government contended in Laird v. Tatum,
408 U.S. 1, 7 (1972), that it had destroyed the "blacklist" and the records in the
computer data bank at Army Intelligence Headquarters, Fort Holabird, Md.,
except for one copy retained for the instant litigation. In his preface to the Staff
Report, supra note 2, at vi, Senator Ervin expressed some doubt whether in view
of the inevitable bureaucratic inertia all copies had in fact been destroyed.

54 S. 3750, 92d Cong., 2d Sess. (1972). The full text of this bill is contained
in 118 Cong. Rec. S 10,256 (daily ed. June 27, 1972). The bill also deals with
the use of the military to execute the laws of the United States or of a state and,
as such, seems to be an amplification of the posse comitatus act, see note 8 supra.
A bill with many identical provisions, H.R. 15,823, 92d Cong., 2d Sess. (1972),
was introduced in the House of Representatives by Representative Abzug on June
Abzug's bill differs from Senator Ervin's in its omission of several provisions, the
principle one of which for our purposes is § 3(c), which permits surveillance of
persons seeking employment with the Department of Defense.
this bill by the recently concluded 92d Congress. It seems extremely likely, however, that Senator Ervin will reintroduce the bill in the 93d Congress.


1. The Weaknesses of DoD Directive 5200.27 and the Ervin Bill

The problem of surveillance of civilians by the military is, in many ways, the most easily resolved of the variety of problems created by Government surveillance. Almost all surveillance of civilians by the military should simply be prohibited, since it is contrary to the traditions of the English and American peoples to give the military any substantial role in law enforcement activities.\footnote{For the congressional expression of this view, see note 8 supra. One might note here also the hostility to the trials of civilians by military tribunals. See Reid v. Covert, 354 U.S. 1 (1957); Ex parte Milligan, 71 U.S. (4 Wall.) 2 (1866); cf. U.S. Const. amend. III.} The ability of Great Britain and the United States to maintain civilian control over the military as well as to avoid the military coups that have troubled so much of the world is undoubted testimony of the soundness of this policy.

Viewed in this light, DoD Directive 5200.27, though clearly a salutary step, is much too broad in terms of the surveillance which it purports to authorize. First, as to the third mission (dealing with anticipated civil disturbances), if the law enforcement capabilities of local and state authorities are inadequate, why should resort first be had to the Department of Defense rather than to the Federal Government's civilian law enforcement agencies? Second, although the authority is considerably circumscribed,\footnote{See DoD Directive 5200.27, supra note 46, IV(C), V(F).} the directive does permit infiltration of civilian organizations and the observation of private meetings by the military in the pursuit of all three missions. Third, while surveillance by way of infiltration of civilian organizations and observation at private meetings requires specific prior authorization by the Secretary or his designee\footnote{Id. V(E), V(F), quoted in text accompanying note 52 supra.}—with the unfortunate exception that local commanders can make this determination in emergencies\footnote{See id. V(F).}—an individual who may be the subject of surveillance, as well as presumably small groups of individuals who are not holding private meetings or are not an "organization," are not granted the same protection when the surveillance is undertaken in support of either the Department's mission to protect DoD functions and [p]rop-
erty" or its "[p]ersonnel security mission."\textsuperscript{58} Fourth, since the Department's first mission includes preservation of discipline, loyalty and morale,\textsuperscript{59} the language of the directive would still permit fairly extensive surveillance of individuals who may only be exercising first amendment rights in trying to influence military personnel. Fifth, even when the integrity of military installations is at stake, the directive is too broad because it imposes no geographical restriction upon the surveillance of civilians that may be authorized. Finally, the directive cuts too wide a swath in the area of "[p]ersonnel security"—applying for civilian employment or even for a commission should not subject an individual to military surveillance.

The Ervin bill unfortunately perpetuates two of these evils. It broadly permits surveillance by the military of civilians in connection with their possible employment by the Defense Department or of private employers with access to classified information.\textsuperscript{60} Additionally, as with the Department of Defense directive, no geographical limitations are imposed on surveillance undertaken to protect Defense Department property.

2. \textit{The Proposed Statute}

The proposed statute attempts to deal with the issue of military surveillance in consonance with the general position taken here that such surveillance—in general—goes against the grain of American principles of government. Thus, the statute provides that no surveillance of civilians by the military in support of its mission of helping to suppress civil disturbance may be taken until the President has ordered the military to help maintain civil order.\textsuperscript{61} In this manner, the statute meets the

\textsuperscript{58} See id. IV(B), IV(C), V(F).
\textsuperscript{59} See id. IV(A)(1).
\textsuperscript{60} Perhaps it should be mentioned that Senator Ervin has tried to protect federal employees in his Federal Employees Privacy Bill, S. 1438, 92d Cong., 1st Sess. (1971), by restricting the information that they can be forced to supply to their employers. This bill passed the Senate on December 8, 1971. See 117 Cong. Rec. S 20,830-46 (daily ed. Dec. 8, 1971), which contains the text of the bill as it passed the Senate and excerpts from the Committee Report (No. 92-554). Unfortunately, this bill died in committee in the House.
\textsuperscript{61} A Proposed Statute: The Freedom from Surveillance Act (Proposed Freedom from Surveillance Act), § 3(a)(1), infra at 898. In addition to the occasions upon which Congress has provided that the military may be so used (see note 8 supra), the President undoubtedly also can use the military in this manner to repel an Invasion against the United States. On the use of the military in the statutorily defined roles, see Note, Federal Intervention in the States for the Suppression of Domestic Violence: Constitutionality, Statutory Power, and Policy, 1966 Duke L.J. 415; Note, Riot Control and the Use of Federal Troops, 81 Harv. L. Rev. 638 (1968). It is possible that the President has some inherent power to
problem posed by DoD Directive 5200.27 which, unlike the Ervin bill, does not require a Presidential order before the military can engage in surveillance in support of its civil disturbance mission. The proposal here goes a step beyond the Ervin bill by imposing the additional requirement of prior authorization by the Secretary of Defense or his designee—defining the scope of such surveillance—before military personnel can engage in the surveillance of civilians in support of this mission; it imposes further requirements whenever general, or extended surveillance, is involved. The proposed statute recognizes, however, as it must, that the President has inherent constitutional authority to protect the United States against hostile acts by foreign powers and to protect national security information against foreign intelligence activities.

Other weaknesses of DoD Directive 5200.27, as well as the Ervin bill, are covered by the statute. For example, under the proposal, application for civilian employment with the Department of Defense, or even for a commission in the Armed Forces of the United States, does not automatically authorize surveillance by the military. If the Defense Department is not satisfied with the information supplied by an applicant, it is required to call in the civil investigatory authorities. Likewise, the statute provides that surveillance of civilian employees outside of a military installation is restricted to suspected criminal activities directly connected with the performance of their official duties. In this regard, more extensive surveillance, if necessary, should be the responsibility of the FBI and other civilian agencies, subject to the various limitations, discussed below, that are placed on the activities of these organizations by the proposed statute. In another troublesome area, the statute imposes geographical restrictions on surveillance for the purpose of protecting the in-use troops for law enforcement purposes in the District of Columbia. For example, on several occasions federal troops have been committed, without any Presidential proclamation, to help maintain order in the District of Columbia under the authority of the Government's inherent power to "protect Government property." Letter from Roger C. Cramton, Asst. Att'y Gen'l, Office of Legal Counsel, to the author, Aug. 3, 1972 (copy on file at the New York University Law Review offices). It is not necessary to resolve any issues which this use of federal troops might raise in this forum or in the context of surveillance, which in many ways is a subsidiary issue. Section 3(a)(1) of the proposed statute speaks in terms of the lawful ordering of the Armed Forces by the President to help maintain civil order pursuant to his "constitutional and statutory authority."

63 See Proposed Freedom from Surveillance Act § 3(b), 3(c), infra at 898-99.
64 Id. § 3(a)(3).
65 For the restrictions placed on the civilian authorities, see text accompanying notes 70-90 infra.
tegrity of military installations. Such surveillance is not permitted unless conducted on military reservations or in their immediate vicinity. In all other cases reliance must be had upon the civilian authorities.

In one important situation the authority granted by the proposed statute is, however, broader than that contained in the directive. The latter flatly prohibits all surveillance by the military of all federal, state and local elected officials. This aspect of the directive appears to be window dressing. If the military is ordered by the President to preserve civil order or if such government official is on a military reservation and is reasonably suspected of being likely to commit a crime, it seems ludicrous to suggest that he cannot be subject to surveillance by the military. The statute here proposed permits surveillance of elected officials in this narrow class of cases.

III

SURVEILLANCE BY CIVILIAN AGENCIES OF THE GOVERNMENT

A. The Need for a Statute

Much more difficult than the question of military surveillance is that of surveillance of the individual by the civilian agencies of the Federal Government. Any kind of broad blanket prohibition is out of the question; surveillance is an essential law enforcement technique. Nevertheless, some regulation is necessary.

This is not, however, an area that lends itself easily to judicial regulation, even if the constitutional basis for judicial intervention were clear, which it is not. What is involved is more than the Government's right to use information gathered in the course of surveillance in a criminal prosecution. Indeed, in the usual case, no such prosecution will ever result. What is involved,

66 Proposed Freedom from Surveillance Act § 3(a)(2), infra at 898.
67 See DoD Directive 5200.27, supra note 46, V(C), quoted in text accompanying note 52 supra. Candidates for elected office are also included in this provision.
68 While "surveillance" involves the observation of the public activities of an individual and the collection and maintenance of publicly available information about an individual, it is hard to pin down any fourth amendment rights that have been violated. Cf. Hoffman v. United States, 388 U.S. 293 (1967). See generally United States v. White, 401 U.S. 745 (1971). Rather, one would have to base his claim primarily on the first amendment, and it is hard to see how a court would be prepared to make any decision granting relief in this area that was not narrowly tied to the facts of the particular case before it. For reference to the Government's position that there are no constitutional protections operative in this area, see text accompanying notes 10, 12 supra.
rather, is the citizen’s right to be free of Government surveillance unless the Government has good grounds for singling him out for special scrutiny. Moreover, an intolerable burden would be placed both on the courts and on the individual citizen if each person who believes he is or may be the object of surveillance felt obliged to seek an injunction from the courts. Equally unpleasant is the possibility of conflict between what one judge might allow and what another might prohibit—a situation hardly conducive to respect either for law or for the judiciary. At the same time, some attempt must be made to define what is meant by surveillance. A definition that would prohibit the casual observations of a policeman walking his beat would be ridiculous. On the other hand, the maintenance of dossiers on people, even when the information is gained from the press and other sources, should be included in any definition and subject to regulation.

Clearly, general standards are called for, and the problems involved are ones for which a general legislative solution is particularly required. Only in this way can the complex issues involved be adequately weighed and an appropriate solution reached. Furthermore, only the Congress has the political and legal power to insure that the Executive complies with the standards that are laid down.

B. The Proposed Statute: Prerequisites for a Satisfactory Solution to the Problem of Surveillance by Civilian Agencies

1. When Is Surveillance Permissible?

The central problem, of course, is to determine those situations when surveillance can be justified. A solution to this problem must necessarily protect the freedom of the individual and

60 The proposed statute, by defining surveillance as the continuous observation of an individual for a period in excess of one-half hour on any one occasion or for 15 minutes on two or more occasions within a 30-day period, recognizes that a policeman walking his beat ought to be permitted to be reasonably curious. See Proposed Freedom from Surveillance Act § 1(b), infra at 895. Such continuous observation would also constitute general surveillance if it were carried on for a period extending over 72 hours. See id. § 1(c).

In testifying about the police activities involved in Donohue v. Dulng, 330 F. Supp. 305 (E.D. Va. 1971), aff’d, 465 F.2d 196 (4th Cir. 1972), one of the witnesses stated that he saw a police car drive by while he was looking for a place to park on the way to hear Allen Ginsberg speak at Virginia Commonwealth University. Id. at 311. This, he testified, so disconcerted him that he immediately went home and has not since attended a public assembly. Id. Testimony of this nature, regarded by the trial judge as frivolous, see id., certainly hurt the plaintiffs on their main claims concerning the photographing of demonstrators, claims which were dismissed by the court. Id. at 312. The decision was affirmed on the narrow ground of the plaintiffs’ lack of standing. Donohoe v. Dulng, 465 F.2d 196 (4th Cir. 1972).
yet be consistent (1) with the Government's need to protect itself from the hostile acts of foreign powers and from overthrow by force, and (2) with the Government's right, indeed duty, to prevent crime. As to this latter goal, people must be able to feel safe in their person and property from the activities of criminals. A nation in which the individual does not feel this sense of security is not one in which freedom can flourish. Therefore, a policy that unreasonably interferes with the Government's legitimate interest in investigating crime is obviously not one that is in the public interest.

As interpreted by the courts, our Constitution quite properly prohibits governmental authorities from arresting a person or searching his home or seizing his papers unless they have "probable cause" to believe that he has committed a crime or that he is in possession of property that may lawfully be seized.\(^70\) When the question involves the Government's right of surveillance of individuals in the course of their public activities (where there is no intrusion into anyone's home or place of physical privacy\(^71\) or physical restraint of anyone's person), the requirement of "probable cause" is probably too stringent. This is particularly so since the Supreme Court, in an opinion written by former Chief Justice Earl Warren, has held that a police officer may "stop and frisk" an individual if the officer reasonably believes that the individual is carrying a concealed weapon—at least when there is reason to believe that criminal activity is afoot—even though the officer does not have probable cause to arrest the individual.\(^72\) In fact, the Court has recently reaffirmed this position and construed it to permit an officer to rely, in some cases, on information supplied by an informant.\(^73\) The scope of any such search is obviously limited to that necessary to discover whether the indi-

---

\(^70\) Since the Supreme Court repudiated the "mere evidence" test in Warden v. Hayden, 387 U.S. 294 (1967), it now appears that evidence of a criminal offense may be seized, even when it is not contraband. See 18 U.S.C. § 3103a (1970). The American Law Institute has proposed, however, that private writings such as diaries and personal letters—with the exception of handwriting samples—should not be subject to seizure during an authorized search and seizure. See Model Code of Pre-Arraignment Procedure § 210.3(2) and accompanying note (Proposed Official Draft No. 1, 1972). See also Commentary, id. at 155-59.


\(^72\) Terry v. Ohio, 392 U.S. 1 (1968).

vidual is armed. While the probable cause standard would, therefore, probably impose too great a burden on law enforcement authorities, there nonetheless must be some limits to the Government's power to engage in surveillance of the public acts of individuals.

The appropriate solution would seem to be to restrict, by statute, the Government's right to engage in surveillance to those situations in which the Government reasonably suspects that the individual or individuals under surveillance have committed or are likely to engage in criminal activity, or in which there is a reasonable possibility that violence is likely to occur even if it is impossible to specify in advance which individual or individuals are likely to commit acts of violence.\textsuperscript{74} Likewise, the Government's right to protect itself against the hostile acts of foreign powers should be recognized, although stated in a manner that does not invite its abuse.\textsuperscript{75} On the other hand, following the Supreme Court's lead in United States v. United States District Court for the Eastern District of Michigan\textsuperscript{76}—rejecting the Government's contention that it could use electronic devices to "conduct warrantless domestic security surveillance" in the interest of national security—no mention has been made in the proposed statute of any inherent power of the President to take action to protect the United States from overthrow by force. Although it would be hard to deny that the President has such power, the authority given by the proposed statute to engage in surveillance when there is reason to believe that a crime will be or has been committed or that violence is likely to occur at a public gathering seems more than adequate to the nation's needs. Finally, certain forms of surveillance should be very tightly controlled. In particular, surveillance of civilians by any government agency at political meetings should be prohibited in all but the most narrowly defined set of circumstances.\textsuperscript{77}

Before leaving this area, mention should be made of the possibility of requiring a prior court order before the Government can engage in surveillance. This requirement would impose a very great burden on the courts, as well as on the Government, and should only be resorted to if it proves impossible to control the law enforcement authorities in any other way.\textsuperscript{78} Nevertheless,

\textsuperscript{74} On this point, see Proposed Freedom from Surveillance Act § 2(a), infra at 896-97.
\textsuperscript{75} For suggested terminology, see id. § 2(d), infra at 898.
\textsuperscript{76} 407 U.S. 297, 303 (1972).
\textsuperscript{77} See Proposed Freedom from Surveillance Act §§ 2(b)-(c), infra at 897-98.
\textsuperscript{78} For the controversy over whether a warrant procedure will be able to confine the search and seizure within reasonable bounds if electronic surveillance
adequate statutory regulation of the Government's surveillance activities requires that extended surveillance of individuals or groups be authorized by officials who can be held politically accountable. The proposed statute thus requires written authorization by the Attorney General or his designee before Government agents can engage in extended surveillance.79

2. Necessity for Placing Good Faith Reliance on Civil Authorities

Any general criteria restricting the Government's right to engage in surveillance must inevitably rely to a large extent on the good faith of law enforcement authorities. Whether a particular subject of surveillance is likely to commit a crime or whether acts of violence are likely to occur is a difficult question, and one that involves a great degree of subjective evaluation. That is why it would be unfair in most instances of mistaken judgment to impose a crippling financial and personal burden—in the form of vulnerability to suit—on the individual officer engaged in the surveillance or even on the person authorizing the surveillance.

Certain considerations which must be taken into account virtually require reliance on the subjective judgment of law enforcement officials. Any statutory standard should try to take cognizance of the fact that the seriousness of the possible crime is certainly a relevant factor and would justify surveillance in situations in which the relative likelihood of the crime would be insufficient to justify surveillance in the case of a minor crime.80 Likewise, the degree of possible physical danger to members of the public is also a relevant consideration.81 Thus, when the likelihood or the severity of the possible danger is of a very high order, surveillance might be justified in situations in which the possible criminal act, in light of the potential penalties for its commission, would only be considered a minor crime and when, in the absence of physical danger, the likelihood of its commission would not be high enough to justify surveillance.82

79 See Proposed Freedom from Surveillance Act § 4(a), infra at 899.
80 See id. § 1(b), infra at 896.
81 See id.
82 The fact that law enforcement authorities must take into account the like-
Despite the necessity of leaving much to the discretion of the law enforcement authorities, a statute can, by specifying the relevant considerations, at least assure that law enforcement officials who perform their duties in good faith will know what criteria to consider; and such a statute can also assist the courts when they are called upon to review the Government's exercise of its surveillance powers. The potential for abuse can be further restricted by a statutory scheme which provides, as does the proposed statute, for a framework for continual congressional scrutiny of the Executive's use of its surveillance authority. 65

3. Surveillance in Connection with Employment

A word should be said about surveillance of applicants for employment with the Federal Government or of defense contractors utilizing classified information. The proposed statute permits the gathering and maintenance of information about an individual when authorized by law. 84 Employment checks would come within this provision. Application for employment by the Federal Government, or even employment by the Government, should not, however, expose an individual to physical surveillance as that term is defined in the statute, unless that person is reasonably believed to have committed or to be likely to commit an offense. 85

4. Penalties

A statutory solution should provide for civil and criminal penalties for failure to comply with its requirements, but only for the most flagrant and willful of such breaches of its provisions. 86 In such cases, a civil action for damages might also be allowed against the United States because, after all, the Government is responsible for the conduct of its agents. 87 Less flagrant and

65 Proposed Freedom from Surveillance Act § 11, infra at 901-02.
64 Id. § 1 (b), infra at 895.
86 See id. § 2 (a), infra at 896-97.
87 See id. §§ 6-7, infra at 900.
88 An action for damages against the United States for violation of individual rights is finding increasing favor. For example, in S. 2657, 92d Cong., 1st Sess. (1971), as amended Dec. 13, 1971, Senator Bentsen proposed to modify the exclusionary rule so as to permit the introduction of illegally seized evidence when the violation of the fourth amendment is not substantial. As part of the statutory
willful failures to comply with the statutory standards, however, should only result in the inability to introduce as evidence, in subsequent criminal prosecutions, any information, or the fruits of any such information, gathered as a result of an unlawful surveillance.\textsuperscript{88} In addition, the Government should not be permitted to keep in its files information obtained as a result of unlawful surveillance.\textsuperscript{89} The proposed statute, however, goes one step further. It defines surveillance to include the maintenance of a file on an individual that is not otherwise authorized by law.\textsuperscript{90} Thus, maintenance of such files—even when the information in them has not been obtained by unlawful surveillance—is only permitted when physical surveillance would be permitted.

C. The Decision to Exclude a Broad-Ranging Regulation of the Government’s Recordkeeping Activities

The subject of governmental files clearly encompasses a vast area of discussion. The possible dangers to the individual in a “dossier society” have been well documented by others\textsuperscript{91} and do not need to be repeated here. Since accurate information is essential for the purposes of modern government, outright prohibition of most forms of governmental recordkeeping is obviously out of the question. What is needed is sensible regulation. The proposed statute, however, is aimed at overt governmental surveillance of individuals primarily by law enforcement agencies. It would be

scheme of S. 2657, a tort action against the United States is allowed for illegal searches and seizures by agents of the United States, with a maximum recovery of $25,000 including actual and punitive damages.

In § 10(a) of the Proposed Freedom from Surveillance Act, infra at 901, an action is permitted against the United States for willful unlawful surveillance of an individual. Although recovery of punitive damages is not provided for, the act permits recovery for actual damages at not less than $100 for each day upon which acts of surveillance prohibited by the statute take place. The justification for not permitting recovery of punitive damages against the United States is that the types of factual situations confronted in cases involving acts of surveillance are likely to be less serious than those involving unconstitutional searches and seizures. Allowance of recoveries of punitive damages against the United States should await further experience under a statute of the type proposed. It should be noted, however, that punitive damages of up to $1,000 are permitted under § 7 of the proposed statute, infra at 900, which imposes a civil penalty against offending federal agents.

\textsuperscript{88} See Proposed Freedom from Surveillance Act § 5, infra at 899-900. The author is fully cognizant in making this proposal that, from the point of view of eliminating prohibited acts of surveillance, an exclusionary rule is not likely to be very effective. See Oaks, Studying the Exclusionary Rule in Search and Seizure, 37 U. Chi. L. Rev. 665, 720-36 (1970).

\textsuperscript{89} See Proposed Freedom from Surveillance Act § 9, infra at 900.

\textsuperscript{90} Id. § 1(b), infra at 895.

\textsuperscript{91} See, e.g., A. Miller, The Assault on Privacy (1971); On Record: Files and Dossiers in American Life (S. Wheeler ed. 1969).
counterproductive to endeavor to include within its scope any large-scale attempt to regulate the Government's recordkeeping activities.

Pending and extant legislation would in any event make the effort to include recordkeeping regulation in the proposed statute a difficult task. The Freedom of Information Act\textsuperscript{92} already permits an individual to obtain access to much of the information about him in Government files. "Investigatory files compiled for law enforcement purposes" are, however, generally excluded from the scope of the Act,\textsuperscript{93} as are matters "required by Executive order to be kept secret in the interest of . . . national defense or foreign policy."\textsuperscript{94} A bill to amend the Act was introduced which would have required the Government to notify a citizen when it intends to open a record on him, to advise him whenever disclosure of any collected information is required by the Freedom of Information Act, to obtain his permission before divulging any part of that record to government agencies or private parties and to allow him to inspect and correct the record.\textsuperscript{95} These provisions did not apply, however, to records "specifically required by Executive order to be kept secret in the interest of the national security," nor to investigatory files compiled by law enforcement agencies except where "such records have been maintained for a longer period than reasonably necessary to commence prosecution or other action."\textsuperscript{96} Of course, these exceptions cover the two areas that most concern us. As limited as were the rights of notification and correction granted by this bill, which its sponsors, Senator Bayh and Representative Koch, entitled a "Citizens Privacy Bill," the bill was not enacted by the 92d Congress. Indeed, no hearings were held on the bill in either House. It is therefore premature now to try to reach the more delicate problem of access and correction of law enforcement files.

There have, however, been other and more hopeful developments in this area. On some matters, for example, the Government has been moving towards a more sensible position as a result

\textsuperscript{93} Id. § 552(b)(7).
\textsuperscript{94} Id. § 552(b)(1).
\textsuperscript{96} S. 975, 92d Cong., 1st Sess. § 5522(d) (1971); H.R. 5974, 92d Cong., 1st Sess. § 552(d) (1971).
of judicial pressure. In response to a decision by Judge Gerhard A. Gesell in *Menard v. Mitchell* \(^{67}\) construing the FBI’s statutory authority to maintain arrest records as permitting only dissemination of such records to law enforcement agencies and to federal agencies for employment purposes, the Government did not seek appellate review; rather, the FBI modified its practices to conform to Judge Gesell’s ruling. \(^{68}\) Congress later temporarily broadened the categories of persons to whom disclosure may be made by including federally chartered or insured banking institutions and, when authorized by state statute and approved by the Attorney General, state and local officials for employment and licensing purposes. \(^{69}\) When the renewal of this authorization came up for consideration, the Senate, at Senator Ervin’s prompting, voted to restrict all dissemination outside of the Federal Government—even to law enforcement agencies—to instances in which the person pleaded guilty, pleaded nolo contendere or was convicted, and that fact is so noted in the record. \(^{70}\) Unfortunately, Senator Ervin’s amendment was eliminated in Conference. \(^{71}\) The Administration itself, however, proposed a bill late in the session that required agencies submitting “criminal record

\(^{67}\) 328 F. Supp. 718 (D.D.C. 1971) (mem.). This decision was rendered following a remand from the court of appeals, 430 F.2d 486 (D.C. Cir. 1970). The suit was brought to compel the Attorney General and the Director of the FBI to remove plaintiff’s fingerprint and arrest records from their files on the grounds that the plaintiff had never been prosecuted for the offense for which he had been arrested. A different district court judge had granted summary judgment for the Government. The court of appeals reversed and remanded for a hearing on the merits. On remand, Judge Gesell found that there was probable cause for the arrest, but adopting a different tack than that of the court of appeals, ruled that the crucial issue was not whether there was probable cause for the arrest but rather who could have access to the information. See 328 F. Supp. at 724–25.


\(^{70}\) Ervin Amendment to H.R. 14,989, Departments of State, Justice, and Commerce, the Judiciary, and Related Agencies Appropriations Bill for 1973. The Senate passed H.R. 14,989 on June 15, 1972. See 118 Cong. Rec. S 9531 (daily ed. June 15, 1972). The text of the Ervin amendment, which was modified in the course of debate, is contained at id. § 9530. For a brief description of other bills dealing with other aspects of this complex problem, see id. at S 9521. For a survey of the law and practice relating to the effect of a criminal record on state and local government employment, see H. Miller, The Closed Door (1972), reprinted in Hearings on H.R. 13,315 Before Subcomm. No. 4 of the House Comm. on the Judiciary, 92d Cong., 2d Sess., ser. 27, at 259-520 (1972).

information," under pain of being denied access to the Government records, to "assure that the information is accurate and complete, and regularly and accurately revised to include subsequent information." This bill permitted dissemination to federal officials, to officials of foreign governments for "visa, security, law enforcement, and employment purposes," to federally insured banking institutions, and to state and local law enforcement agencies for law enforcement purposes or such other purposes "necessitated by State statute" and approved by the Attorney General. In the case of distribution to state or local law enforcement authorities for "other than law enforcement purposes," the individual concerned was given a right to review the information and to dispute its accuracy. Civil and criminal penalties were provided for the willful violation of the Act. This bill was introduced too late in the second session of the 92d Congress for any action to be taken on it in 1972. It appears highly probable, however, that it will be reintroduced in the next Congress, particularly because Senator Ervin has already given notice that he intends to pursue the substance of his proposal at that time. These are all efforts that should be applauded. The important consideration, in addition to restricting access, is accuracy and completeness of information. By making the completeness of information and a requirement of conviction or its equivalent conditions for dissemination outside of the Federal Government, Senator Ervin's proposal may well be more effective than that of the Administration. The latter has more elaborate provisions, but it might prove more difficult to secure compliance with these provisions.

The Federal Government seems to be on the way to striking the proper balance between the individual's privacy and the interests of the state in this area. Therefore, at this time, there

---

894 NEW YORK UNIVERSITY LAW REVIEW [Vol. 47:871

---

802 S. 3834, 92d Cong., 2d Sess., para. (b) (1972). The bill was introduced by Senator Bentsen on July 24, 1972 at the Administration's request, and was in the form of an amendment to 28 U.S.C. § 534 (1970), which governs acquisition, exchange and use of "identification information and records."

803 S. 3834, 92d Cong., 2d Sess., para. (c) (1972).

804 Id. at para. (c).

805 Id. at para. (f). In addition, the Attorney General can terminate further dissemination for improper use or disclosure. Id. at para. (d).


807 In contrast, a recent state court decision appears to go too far. The court in Eddy v. Moore, 5 Wash. App. 334, 487 P.2d 211 (Cl. App. 1971), petition for review denied, 79 Wash. 2d 1013 (1971), took the position that a person who is acquitted of a criminal charge should have his arrest and fingerprint records returned to him. But cf. United States v. Reen, 343 F. Supp. 804 (S.D.N.Y. 1972). It seems to this writer that when the proper amount of confidentiality is maintained, including strict control of dissemination, and reasonable efforts are made
does not appear to be any need to make explicit provision for such records, when authorized by law, in the proposed statute. The statute, in any event, is primarily concerned with other problems.

IV

A PROPOSED STATUTE: THE FREEDOM FROM SURVEILLANCE ACT

Section 1. Definitions and Rules of Construction. (a) The definitions set forth in this section are applicable for the purposes of this act.

(b) The term “surveillance” means the continuous observation of any particular subject of surveillance, whether an individual or a single group of individuals or the members of a single organization, for a period of more than 30 minutes on any one occasion or for more than 15 minutes on two or more occasions within any 30-day period. It shall also be deemed to include the maintenance in any file of any information on an individual or a single group of individuals or an organization or its members, the gathering and maintenance of which information is not otherwise authorized by law, regardless of how brief were the observations on the basis of which the information in such files was obtained and regardless of whether the information in such files was obtained by observations or other data-collecting activities performed by officers, employees, or agents of the United States or was obtained from other sources. Each entry of information in any such file shall be deemed to be one “act of surveillance” as that term is used in this act.

(c) The term “general surveillance” means the surveillance of any individual or single group of individuals or the members of a single organization over a period in excess of 72 hours.

(d) The term “offense” means any conduct or activity pro-

---

108 The maintenance by the Government of standard reference works similar to Who’s Who in scope and purpose, however, would not be considered “surveillance” under the proposed statute. Such materials are not “files.”
hibited by any statute, ordinance, or regulation of the United States or of any State or political subdivision thereof for which prosecution is not barred by a previous conviction or acquittal or other attachment of jeopardy or by a statute of limitations.\textsuperscript{169}

(e) The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico and any territory or possession of the United States.

(f) The term “political meeting” shall be deemed to include any meeting at which candidates for public office are chosen or a principal purpose of which is to permit candidates in a primary election or in a general election to address the public and/or to answer questions from the public.

(g) The term “military installation” means any building, property, ship, or aircraft under the direct control of the Department of Defense or of any of its components.

(h) In deciding whether there exist “reasonable grounds to believe” that an individual or group of individuals is “likely to commit an offense,” but not in deciding whether there exist “reasonable grounds to believe” that an individual or individuals have committed an offense, the factors that may be taken into consideration may also include an evaluation of the seriousness of the possible offense, the likelihood of its involving a threat to the physical safety of the person or property of others, and the number of persons the physical safety of whose person or property is likely to be affected. When the surveillance of an individual is sought to be justified on the grounds that an organization to which he belongs is likely to commit an offense the same factors shall be taken into account: \textit{Provided}, that, when surveillance of an individual is justified solely on the grounds that he belongs to an organization that has committed an offense or is likely to commit an offense, the degree of active involvement of the individual in the affairs of the organization as well as the extent of his commitment to the goals of the organization shall also be taken into account.

Section 2. Prohibited Activities. (a) No officer, employee, or agent of the United States shall authorize, or engage, in the

\textsuperscript{169} Surveillance by federal agents when state offenses are involved is permitted because it is often difficult initially for law enforcement officers to tell whether suspected criminal activity concerns federal or state law, and federal agents have an obligation to cooperate in the enforcement of state law as indeed, to some extent, do private citizens.

Imaged with the Permission of N.Y.U. Law Review
surveillance of any individual or group of individuals or the members of any organization unless he has reasonable grounds to believe\textsuperscript{110} that the individual or individuals under surveillance or the organization whose members are under surveillance have committed an offense or are likely to commit an offense.

(b) No officer, employee, or agent of the United States shall authorize, or engage in, surveillance at any meeting held in a public place unless he has reasonable grounds to believe that there are persons present at that meeting whose surveillance is permitted by subsection (a) of this section or that acts of violence are likely to occur at that meeting or in the immediate vicinity of the meeting, or that interference with the orderly processes of government or with any vital public service are likely to occur as a consequence of the meeting: Provided, that nothing in subsections (a) and (b) of this section shall authorize surveillance at any political meeting because of the presence at any such meeting of persons reasonably believed to be likely to commit an offense unless there are also reasonable grounds for believing that any such persons are likely to commit an offense at the meeting or in the immediate vicinity of the meeting during the time at which the meeting is being held; provided further, that nothing in subsections (a) and (b) of this section shall prohibit the attendance at any meeting of whatever description of any officer, employee, or agent of the United States whose attendance at that meeting is for the principal purpose of protecting, as authorized by law, the security of any person lawfully attending the meeting or participating in the meeting.

(c) Whenever surveillance at any meeting or at any political meeting is permitted by subsections (a) and (b) of this section, no records of surveillance shall be maintained with regard to any individual present at the meeting unless there are reasonable grounds to believe that the individual has committed an offense or is likely to commit an offense, except that in the course of reporting on the surveillance of persons whose surveillance is permitted by this act minimal information identifying the persons with whom they came in contact

\textsuperscript{110} The use of the verb "suspects" is an alternative. It is weaker, but it may be more likely to attract the broad spectrum of political support necessary to enact this type of legislation. Parallel changes would have to be made in §§ 1(h), 2(b), and 3(a)(3).
may be included where such information is essential for the accuracy and utility of that report.

(d) Nothing contained in this act shall limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.

Section 3. Surveillance by Military Personnel. (a) No member of the Armed Forces of the United States shall engage in the surveillance of any civilian nor shall any officer, employee, or agent of the United States authorize any such surveillance by members of the Armed Forces of the United States unless

(1) the Armed Forces of the United States have been lawfully ordered by the President to help maintain civil order pursuant to the President's constitutional or statutory power to repel invasion or to suppress insurrection or domestic violence or to enforce the Constitution or laws of the United States, or to protect the rights, privileges, or immunities of the people of the United States, and then only in connection with the maintenance of such civil order;

(2) such surveillance takes place on a military installation or in the immediate vicinity of a military installation; or

(3) such surveillance concerns a civilian employee of the Armed Forces of the United States, but then only when such civilian employee is reasonably believed to have committed or is likely to commit an offense and when such offense directly relates to his employment by the Armed Forces of the United States.\(^1\)

(b) Whenever surveillance of civilians is permitted by subsection (a)(1) of this section, no member of the Armed Forces of the United States shall engage in any such surveillance nor shall any officer, employee, or agent of the United States authorize such surveillance unless the Secretary of Defense or his designee has granted prior written

\(^1\) Although the Department of Defense has no prosecutorial responsibility for such offenses, surveillance for this purpose is likely to take place both on and off a military installation, and it seems too cumbersome to require bifurcation of the surveillance function between civilian and military authorities.
authorization describing the scope and purpose of such surveillance, except in bona fide emergencies in which case such surveillance shall be immediately reported to the Secretary of Defense or his designee and written authorization obtained for any further surveillance.

(c) No general surveillance, as that term is defined in this act, shall be undertaken pursuant to the authority granted in subsection (a) of this section without the prior written authorization of the Secretary of Defense or his designee. The Secretary shall keep records of the occasions upon which authorization to engage in general surveillance has been authorized by him or his designee, which records shall, as nearly as possible, conform to the requirements imposed upon the Attorney General by this act, and, unless the Secretary chooses to make an annual report to the Congress, such records shall be available upon request to members of the Congress.

Section 4. General Surveillance. (a) No officer, employee, or agent of the United States shall engage in the general surveillance, as that term is defined in this act, of any individual or group of individuals or the members of any organization unless such surveillance has been authorized in writing by the Attorney General or by an Assistant Attorney General designated by the Attorney General, but no more than two Assistant Attorneys General may be designated to exercise this power concurrently.

(b) All such written authorizations shall be kept on file at the Department of Justice in Washington, D.C.

(c) No authorization to engage in surveillance granted by the Attorney General or any of the Assistant Attorneys General designated by him shall be valid for a period greater than six months from the date of its issuance. 122

(d) No authorization to engage in general surveillance may be renewed unless the offense or potential offense to which it relates is punishable by death or by imprisonment for more than one year.

Section 5. Violation of this Act. Subject to the provisions of section 3504, chapter 223, title 18, United States Code, no

122 While some may consider six months too long a period of time, the strict limitation on renewals contained in § 4(d) of this proposed statute should be taken into account. A more limited period of initial surveillance would require a less stringent renewal policy.
information secured as a result of a violation of this act nor the fruits of any such information secured as a result of a violation of this act shall be admissible in evidence against any individual in any criminal prosecution in the courts of the United States or in the courts of any State or political subdivision thereof.

Section 6. Willful Violation. Any officer, employee, or agent of the United States who willfully violates any of the provisions of this act shall be fined not more than $500 or imprisoned not more than six months, or both.

Section 7. Civil Penalty. Any officer, employee, or agent of the United States who willfully violates any of the provisions of this act shall be liable to any person who, as a result of any such violation of the provisions of this act, has been the subject of surveillance prohibited by this act in an amount equal to the sum of—
(1) any actual damages suffered by the plaintiff as a result of surveillance prohibited by this act, but not less than liquidated damages at the rate of $100 a day for each day during which acts of surveillance prohibited by this act took place;
(2) such amount of punitive damages as the court may allow, but not in excess of $1,000; and
(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorneys' fees as determined by the court.

Section 8. Jurisdiction of Courts; Limitation of Actions. An action to enforce any liability created under this act may be brought in any appropriate United States district court without regard to the amount of controversy within two years from the date on which the liability arises.

Section 9. Prohibition of Records. No information obtained as a result of any violation of this act shall be kept in any files maintained by any department or agency of the United States, nor shall any information obtained as a result of any violation of this act be furnished or divulged to any person or to any department or agency of the United States or of any State or political subdivision thereof.
Section 10. Civil Action Against the United States. (a) Whenever any officer, employee, or agent of the United States has violated any of the provisions of this act, any person who, as a result of any such violation of this act, has been the subject of a surveillance prohibited by this act may bring a civil action against the United States, to secure, where appropriate, the following relief:

(1) the deletion from any file or files kept by any department or agency of the United States of any information gathered as a result of any surveillance prohibited by this act;

(2) in the case of a willful violation of any provision of this act, the recovery of any actual damages suffered by the plaintiff as a result of surveillance prohibited by this act but not less than liquidated damages at the rate of $100 a day for each day during which any acts of surveillance prohibited by this act took place; and

(3) in the case of any successful civil action to secure relief under this section, the costs of the civil action together with reasonable attorneys' fees as determined by the court.

(b) Any suit seeking relief under subsection (a)(1) of this section or any action for damages in which relief under subsection (a)(1) of this section is also sought shall be brought in the district court in the judicial district in which such files are kept. Any other action for damages under this section shall be brought in the district court in the judicial district in which the plaintiff resides or in which any of the unauthorized acts of surveillance took place.

(c) Any action for damages against the United States under this section shall be brought within two years from the date on which the liability arises and all such actions shall be tried by the court without a jury.

Section 11. Report to the Congress. The Attorney General shall submit a written report to the Congress by January 31st of each year describing the number of general surveillances that were authorized during the preceding calendar year. Such report shall indicate, in reasonable detail for each such category, the categories of suspected offenses for which general surveillances were authorized and, for each such category, the number of authorizations to engage in general surveillance that were renewed during the preceding calen-
dar year. Such report shall also include, for each such category, a statement as to the number of (1) initial authorizations and (2) renewals of authorization to engage in general surveillance that were issued during the preceding calendar year by each person entitled under this act to grant such authorization.

V

Conclusion

The proposed statute seeks to fulfill the criteria outlined in this article. It represents an attempt to construct a responsible solution to the general problem of surveillance by the Federal Government of individuals and groups in our society. It is hoped that the statute might also serve as a model for legislative action by the states. In closing, it is the draftsman’s wish that the proposed statute be read critically, for this article has no other purpose than to initiate a public discussion that will result in law reform that is in the best interest of the country.